(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 840 533 A1

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
25.02.2015 Bulletin 2015/09

(51) Int Cl.:
G06Q 10/00 *(2012.01)* ***G08B 25/14*** *(2006.01)*

(21) Application number: **14179942.9**

(22) Date of filing: **05.08.2014**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME

(30) Priority: **16.08.2013 US 201313968494**

(71) Applicant: **Honeywell International Inc.**
Morristown, NJ 07962-2245 (US)

(72) Inventors:
- **Dharmalingham, Vinoth**
  Morristown, NJ New Jersey 07962-2245 (US)
- **Krishnan, Viswanathan Chatapuram**
  Morristown, NJ New Jersey 07962-2245 (US)
- **Venkatesh, Vinay**
  Morristown, NJ New Jersey 07962-2245 (US)
- **Popowski, Paul M.**
  Morristown, NJ New Jersey 07962-2245 (US)

(74) Representative: **Houghton, Mark Phillip**
Patent Outsourcing Limited
1 King Street
Bakewell, Derbyshire DE45 1DZ (GB)

(54) **System and method for virtual region based access control operations using bim**

(57) A system operates using the steps of a building information model (BIM) of a security system defining a three-dimensional floor plan of a secured area, the BIM receiving an a graphical input from a user defining at least one subarea of the secured area, a user input of the security system receiving a selection of the at least one subarea of the secured area, the user input of the security system receiving a change in a parameter from the user of the security system, the parameter is used by a plurality of security devices within the at least one subarea and changing a corresponding parameter within each of the plurality of security devices to match the changed parameter.

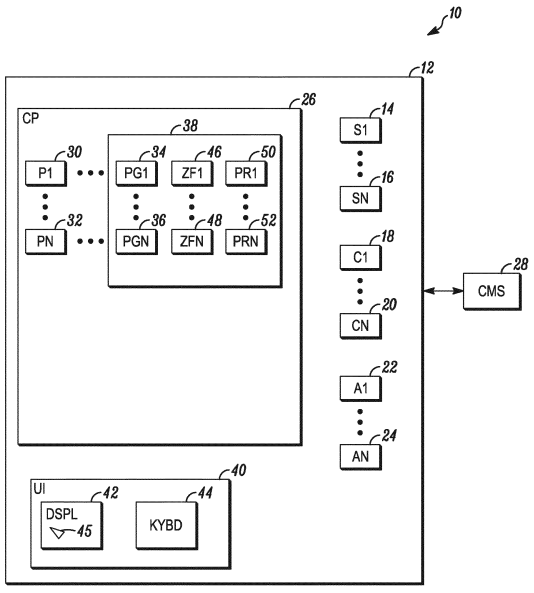


FIG. 1

EP 2 840 533 A1

Description

FIELD

[0001] The field of the invention relates to security systems and more particularly to methods of administering to the operations of such systems.

BACKGROUND

[0002] Security systems are generally known. Such systems are typically used for the protection of people and assets within a secured area.

[0003] In many cases, the secured area is surrounded by some sort of physical barrier (e.g., a fence, wall, etc.) with one or more access doors for entry and egress of authorized users. A sensor may be provided on each door and window in order to detect intruders.

[0004] The sensors may be monitored by a security controller. Upon activation of one of the sensors, the controller may transmit an alarm message to a central monitoring station. The central monitoring station may respond by summoning the police.

[0005] At least some of the doors may be provided with an input device that may be used by authorized users of the secured area to provide inputs to the security controller. Inputs may include commands to arm or disarm the security system, to arm or disarm certain doors or simply to allow the user to pass through an associated door without triggering an alarm.

[0006] While existing security systems work well, they are difficult to administer where the number entry points, sensors and types of sensors number in the hundreds and especially where they are used across multiple time zones. Accordingly, a need exists for better methods of administering large security systems.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007]

FIG. 1 is a simplified block diagram of a security system shown generally in accordance with an illustrated embodiment;

FIG. 2A is a block diagram of a prior art system;

FIG. 2B is a block diagram of a system as in claim 1;

FIG. 3 is a display provided by the system of FIG. 1;

FIG. 4 is a set of steps that may be used by the system of FIG. 1; and

FIG. 5 is an alternate set of steps that may be used by the system of FIG. 1.

DETAILED DESCRIPTION OF AN ILLUSTRATED EMBODIMENT

[0008] While embodiments can take many different forms, specific embodiments thereof are shown in the drawings and will be described herein in detail with the understanding that the present disclosure is to be considered as an exemplification of the principles hereof, as well as the best mode of practicing same. No limitation to the specific embodiment illustrated is intended.

[0009] FIG. 1 is a simplified block diagram of a security system 10 shown generally in accordance with an illustrated embodiment. Included within the security system is a number of sensors 14, 16 or a number of sensors 14, 16 and cameras 18, 20 used to detect security threats within a secured area 12. The secured area may be located at a single geographic location as shown in FIG. 1 or may be a number of geographically separate areas connected by a communication connection.

[0010] The sensors may include one or more switches coupled to the doors and windows around a periphery of the secured area. The sensors may also include one or more passive infrared (PIR) detectors that are able to detect the movement of intruders within an interior of the protected space. Alternatively, the sensors may also include one or more environmental sensors (e.g., smoke detectors, carbon monoxide detectors, natural gas detectors, etc.).

[0011] The system may also capture images for security purposes from one or more cameras 18, 20. The cameras may be used to record events from within the secured area or (with the appropriate processing capability) may also be used to detect threats such as posed by intruders within the protected space.

[0012] The secured area may also include one or more actuator devices (actuators) 22, 24. The actuators may selected from any of a number of different types of devices. For example, at least some of the actuators may be audio and/or visual devices (e.g., a siren or siren and flashing light) that announces the detection of a threat within one or more of the secured areas or subareas. Alternatively, the actuators may include one or more linear actuators that open/close doors. At least some of the actuators may also be provided that activate sprinklers that quench fires or that activate or deactivate fans that clear smoke from an area or subarea.

[0013] The secured area may also include combinations of sensors and actuators that operate cooperatively to achieve a security objective. For example, at least some of the sensor and actuator combinations may include a card reader used in conjunction with a door lock. In this case, the card reader reads an identification card of a person authorized to use some part of the secured area and activates the lock to allow entry by that person into and out of that part of the secured area.

[0014] Included within the secured area or within a central monitoring station 28 may be a control panel 26. The control panel operates to monitor the sensors and cameras and to control the actuators in accordance with a predetermined security plan.

[0015] Associated with the control panel is a user interface (UI) 40. The user interface may include an interactive display 42 using a touch-sensitive screen or may be embodied as a conventional display 42 with a separate

keyboard 42.

[0016] Included within the control panel may be one or more processor apparatus (processors) 30, 32, where each operates under control of one or more computer programs 34, 36 loaded from a non-transitory computer readable medium (memory) 38. As used herein, reference to a step of a computer program is also reference to the processor that executed that step.

[0017] In general, the secured area operates under control of a three-dimensional (3D) building information model (BIM) embodied at least as data and data structures within memory. In this context, each sensor, camera and actuator is associated with a respective geographic location within the BIM. More specifically, each sensor, camera and actuator has a set of coordinates associated with the device that defines where the device is located within the BIM model.

[0018] The use of the BIM offers a number of advantages in the execution of the security plan. For example, a BIM processor may be used to display three dimensional models of the secured area on the user interface. Since the BIM also includes a respective coordinate of each sensor, camera and actuator, the BIM processor is able to superimpose the location of each of each sensor, camera and actuator on 3D images.

[0019] The secured area may be divided into a number of subareas, each with a separate security control subsystem. For example, upon activation of the control panel, one or more of the processors within the control panel would operate to discover each sensor, camera and actuator within the secured area based upon a class of the device. For example, intrusion sensors may constitute or otherwise define a first class of device that would be discovered by an intrusion processor. Similarly, cameras would define a second class of device that would be discovered by a processor that processes information from the camera and that would also operate to control certain aspects (e.g., pan-tilt-zoom (PTZ)) of the camera. The processor that discovers cameras may be referred to as a camera processor/controller or simply as a camera controller. Similarly, card readers and associated lock actuators would define a third class of device discovered by a reader controller. Actuators would define a fourth class of device discovered by an actuator controller.

[0020] Each class of device operates under a respective set of parameters. Each of the set of parameters represents an input to that particular class of device that controls the output of the device or the way the output is provided.

[0021] In general, each class of device has a first set of parameters that are unique to that device and a second set of parameters that are common with other classes of devices. An example of the second set of parameter includes a value of time (e.g., Greenwich mean time). An example of the first set of parameters that are not common with other classes of devices may include the frames per second set by the camera controller in receiving images from the camera, the PIN numbers of authorized users used by the card reader controller, etc. Because of the differences in operating parameters, each class of device may be considered as functioning under its own localized control system or control panel.

[0022] Once activated, the user could define a set of operating parameters for each class of device on an individual basis and globally. For example, the user could define a global clock that would be maintained and used by each control system. The user may also define a set of time related thresholds for at least some classes of device. For example, the user may define a time in the evening when images from the camera would be saved into an archive for later use if a crime were subsequently detected and where the security system sensors did not detect the crime.

[0023] Similarly, the user could also define a set of rules for each class of device. Rules in this case represent a broader category of parameters. For example, a rule may define a combination of parameters used by a processor class of device the produce a particular output. For example, a rule may specify that during a first time period, a camera may simply record video and during a second time period a camera may perform motion detection. In this case, the first set of parameters include a definition of the first time period (start and stop times) and a triggering parameter that causes the recording of video during the first time period. The second set of parameters include the definition of the second time period (start and stop time) and triggering parameter that activates a corresponding program to cause motion detection and reporting of motion as an alarm state.

[0024] Each class of device has a set of parameters that define that class of device. For example, a camera may have a first parameter that defines whether the camera records video frames to memory and a second parameter that defines whether the camera performs motion detection. The camera may also have another parameter that defines when the camera performs each function.

[0025] Similarly, a card reader/door lock combination may have a set of parameters that activate and deactivate a corresponding set of rules for that device. In general, an identifier of each class of devices defines how that device operates and the parameters that activate and deactivate the functions of that device. Since the devices in each class have substantially identical functions in terms of the behaviors that may be exhibited by the device, the rules followed and the thresholds for those behaviors and rules, the functions of each device may be defined by a parameter file 50, 52 for that device. It should be noted in this regard that since the devices in any one class have substantially identical functions, the format of the parameter file of each devices within a class is also identical. The common format of parameter files among devices of the same class allows the use of a copy paste function that allows the behavior, rules and thresholds of one device in a class to be copied into another device within the same class.

[0026] Under the BIM, a user may the BIM processor to divide the secured area 100 into two or more subareas 102, 104, 106 (see for example, FIG. 2B). Dividing the secured area into subareas also causes the control panel to divide the control systems of the secured area into a respective set of control systems for the subareas.

[0027] In order to divide the secured area, the authorized user may activate a BIM icon on the display 42 of the user interface. The user may then identify one or more subareas, regions or security zones within the secured area by tracing the outline of each subarea using the cursor 45. The user may complete the process by activating an ENTER button on the keyboard 42 or activating a COMPLETE softkey on the display to create the virtual regions.

[0028] In general, this process is used to define a number of virtual regions under a coordinate system defined by the BIM. This process may be repeated any of a number of times as the user creates the virtual regions using the process of FIG. 2. As each zone is created, it is stored into a respective zone file 46, 48.

[0029] The creation of a number of subareas may be used as a method of creating a hierarchy of control systems and operating parameters. The hierarchy allows the system to internally group the devices in each virtual area based upon the class of the device. For example, the highest level (i.e., associated with the entire secured 12) represents a set of global operating parameters. Those subareas that have been divided out can be independent changed by the user. This is important because the highest level can be used to define a global time while the subareas can have a time value that is offset based upon the time zone in which the subarea is located. In this regard, the end user can directly click on a virtual region and can change the time zone. In response the system will internally apply the modified time zone to all readers and panels in that virtual region. Similarly, security settings and rules can be defined on a global scale and on a local scale.

[0030] In one embodiment, the security settings (and parameters) of a parent area may be copied into a created virtual subarea. Once created, the user can select the subarea (via the cursor) and adjust parameters of the created virtual subarea at will.

[0031] For example, each virtual subarea may have a user input including a set of function buttons 300. Once function button (e.g., 302) may be provided to adjust global parameters (e.g., time) for that region. Other function buttons (e.g., 304) may be used to select a particular class of device for that region. Other function buttons may be used to select parameters and to change the respective parameters.

[0032] For example, the end user may use a first portion of a user input to click on virtual region 1 and a second portion of the user input to choose the "copy region settings" option (FIG. 5). In this regard, a BIM processor may display virtual region 1 along with a set of options related to region 1. One of the options may be the "copy region settings" option. Following this step, the end user may right click on region 2 and choose the "paste" option. In response, a parameter processor of the system copies the regional settings of region 1 into region 2. Now all of the settings that have been previously applied to virtual region 1 will be replicated into region 2.

[0033] FIG. 2 compares the system described herein with prior systems. For example, prior systems (FIG. 2A) only allowed a user to access the system on a global level (level 1). If a user should wish to change a parameter, the user would need to access a particular control system associated with a particular class of device (level 2). However, this particular control system included all of the devices of that class throughout the system. Once the user has selected a particular control system (i.e., class of device), the user would be given access to the devices on level 3.

[0034] In contrast, FIG. 2B shows that once a user selects a particular subarea, the user only has access to the devices) within that subarea. In this regard, once a user clicks on a particular region or zone, the system may present a number of classes of devices as shown on level 2 and FIG. 3. One class may be a time keeper class of device. Other classes may include sensors, cameras or card readers. In addition (and as shown in FIG. 3), the selection of a region shows the 3D image of the device under the BIM along with the status of each device within that region. This allows for much simpler administration of the security system.

[0035] The prior system of FIG. 2A requires that the end user to have complete knowledge of the devices in order to perform any action on the system. This increases the cost of the system by requiring that any user have complete training regarding the system and increases the possibility of mistake.

[0036] For example, consider the instance in which an end user wants to change the time zone for a particular area in the secured area. Since the secured area is embodied as a single logical entity, the user would have to change the time zone for each device (e.g., each card reader) within the particular area. This is a repetitive operation that would need to be done on all readers within the particular area.

[0037] Similarly, consider the instance in which a door forced open alarm occurred near a building monitoring station (BMS) room and the end user is interested in viewing the recorded video of any camera mounted near the BMS room. In this case, the end user has to know the geo location of each camera within a list of cameras in order to quickly identify the proper camera.

[0038] The system of FIGs 1 and 2B enables the user to make global changes (i.e., to the extent of the devices located within that subarea) by allowing them to virtually mark any area in the BIM 3D floor plan. This allows the user to directly perform all operations (e.g., rules and policy setting, grant/deny access, changing time zone, etc.) only on that subarea. The devices falling within that virtual area will be grouped for that region and all the

subsequent parameter change operations on that region will reflect back on all the contained devices to the extent they are a global change for that subarea or in the class of device selected for the change.

[0039] In this way, the end user can define the different behaviors, rules, settings, etc. for every virtual region in accordance with the need. This has the effect of completely abstracting the lower level devices and other non-operator centered details in the system and makes inputs to the system more meaningful. The system completely eliminates the need for the operators about the readers, panels and all other low level device details. This helps the end users to more easily and effectively make changes in the operation of the system.

[0040] Whenever changes are made on the virtual regions, like changing a time zone, the system will internally apply all of those changes to the panels/readers in that region. This imparts a logical and physical mapping to the virtual areas that allows a user to visually operate on those regions.

[0041] In a particular example, consider a secured area having a number of security areas, each with a different need for security. With the proposed solution, the operator can draw virtual regions containing different regions (e.g., a datacenter and BMS in one region and another region containing a library and pantry). Now the operator can directly set rules and perform other access control operations directly on the different virtual region as separate operations. This method provides complete flexibility over the access control system and allows the end users to easily configure and segregate the different areas in one region.

[0042] Consider the example where a fire emergency occurs in a particular area of a premises and where for precautionary reasons, the operator should take countermeasures. With the display of a conventional security panel there is no apparent way for the operator to visually look at the display and inherently know the identifiers of nearby regions so that he/she can activate the sprinklers in in those nearby regions or take some other precautionary measure. Unless the operator has complete knowledge of the floors/remises /building structure he/she cannot act immediately in response to emergency situations.

[0043] Consider the example where a secured area has a number of zones with similar security requirements, where different rules and behaviors have been applied among the zones and where at least one of the zones has a rule set that works particularly well. If the operator wants this same set of behaviors, rules and settings to be replicated into another zone or into a newly created zone, then (under illustrated embodiments) the operator is able to directly copy all zone based settings using a simple copy/paste function available through the user interface.

[0044] The system offers a number of advantages over prior methods. For instance, the system completely eliminates any need for the operator to know the lower level device detail of each zone and instead provides the operator with a system wherein device detail is abstracted in a way that is flexibly implemented across adjacent zones. The allows an operator to make changes very quickly and efficiently. Since the system internally takes care of correlating layouts among zones, human errors are prevented.

[0045] In general, the system operates using the steps of a building information model (BIM) of a security system defining a three-dimensional floor plan of a secured area, the BIM receiving an a graphical input from a user defining at least one subarea of the secured area, a user input of the security system receiving a selection of the at least one subarea of the secured area, the user input of the security system receiving a change in a parameter from the user of the security system, the parameter is used by a plurality of security devices within the at least one subarea and changing a corresponding parameter within each of the plurality of security devices to match the changed parameter.

[0046] Alternatively, the system includes a security system having a secured area, a building information model (BIM) of the security system that defines a three-dimensional floor plan of the secured area, a zone file that defines a plurality of zones within the secured area in accordance with a coordinate system of the BIM, a user input of the security system that receives a selection of the at least one zone of the plurality of zones within the secured area, the user input of the security system that receives a change in a parameter from the user of the security system, the parameter is used by a plurality of security devices within the selected zone and a processor that changes a corresponding parameter within each of the plurality of security devices to match the changed parameter.

[0047] In another embodiment, the system includes a security system having a secured area, a building information model (BIM) of the security system that defines a plurality of regions within the secured area, a first portion of a user input of the security system that receives a selection of the at least one region of the plurality of regions within the secured area, a second portion of the user input of the security system that receives a change in a parameter from the user of the security system, the parameter is used by a plurality of security devices within the selected zone and a parameter processor that changes a corresponding parameter within each of the plurality of security devices to match the changed parameter.

[0048] From the foregoing, it will be observed that numerous variations and modifications may be effected without departing from the spirit and scope hereof. It is to be understood that no limitation with respect to the specific apparatus illustrated herein is intended or should be inferred. It is, of course, intended to cover by the appended claims all such modifications as fall within the scope of the claims.

Claims

1. A method comprising:

   a building information model (BIM) of a security system defining a three-dimensional floor plan of a secured area;
   the BIM receiving an a graphical input from a user defining at least one subarea of the secured area;
   a user input of the security system receiving a selection of the at least one subarea of the secured area;
   the user input of the security system receiving a change in a parameter from the user of the security system, the parameter is used by a plurality of security devices within the at least one subarea; and
   changing a corresponding parameter within each of the plurality of security devices to match the changed parameter.

2. The method as in claim 1 further comprising selecting at least some of the plurality of devices based upon a class of the device where class defines at least in part a function of the device.

3. The method as in claim 2 wherein the parameter further comprises a local time.

4. The method as in claim 1 wherein the parameter further comprises an activation time.

5. The method as in claim 1 wherein the parameter further comprises an identifier that defines at least one authorized user of the security system.

6. The method as in claim 1 wherein the parameter further comprises an access condition.

7. The method as in claim 1 wherein the change in the parameter is defined by copying a set of rules from one subarea and pasting the copied set of rules into another subarea.

8. A system comprising:

   a security system having a secured area;
   a building information model (BIM) of the security system that defines a three-dimensional floor plan of the secured area;
   a zone file that defines a plurality of zones within the secured area in accordance with a coordinate system of the BIM;
   a user input of the security system that receives a selection of the at least one zone of the plurality of zones within the secured area;
   the user input of the security system that receives a change in a parameter from the user of the security system, the parameter is used by a plurality of security devices within the selected zone; and
   a processor that changes a corresponding parameter within each of the plurality of security devices to match the changed parameter.

9. The apparatus as in claim 8 further comprising a user interface that receives a selection of at least some of the plurality of devices based upon a class of the device where class defines at least in part a function of the device.

10. The apparatus as in claim 9 wherein the parameter further comprises a local time.

11. The apparatus as in claim 8 wherein the parameter further comprises an activation time.

12. The apparatus as in claim 8 wherein the parameter further comprises an identifier that defines at least one authorized user of the security system.

13. The apparatus as in claim 8 wherein the parameter further comprises an access condition.

14. The apparatus as in claim 8 wherein the change in the parameter is defined by copying a set of rules from one subarea and pasting the copied set of rules into another subarea.

15. A system comprising:

   a security system having a secured area;
   a building information model (BIM) of the security system that defines a plurality of regions within the secured area;
   a first portion of a user input of the security system that receives a selection of the at least one region of the plurality of regions within the secured area;
   a second portion of the user input of the security system that receives a change in a parameter from the user of the security system, the parameter is used by a plurality of security devices within the selected zone; and
   a parameter processor that changes a corresponding parameter within each of the plurality of security devices to match the changed parameter.

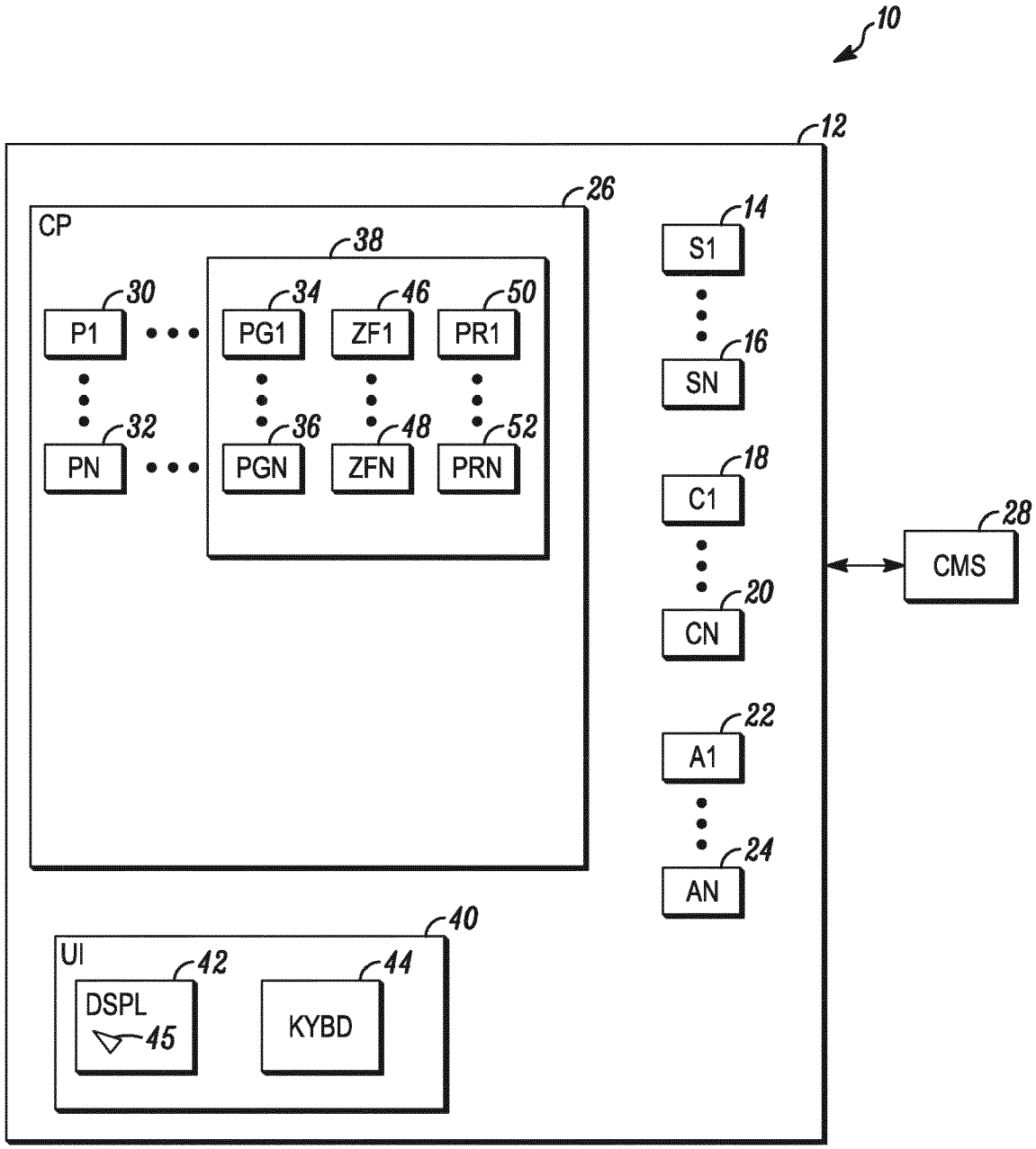

10
12
26
CP
38
30
P1
PN
32
34
PG1
PGN
36
46
ZF1
ZFN
48
50
PR1
PRN
52
14
S1
SN
16
18
C1
CN
20
22
A1
AN
24
28
CMS
40
UI
42
DSPL
45
44
KYBD

FIG. 1

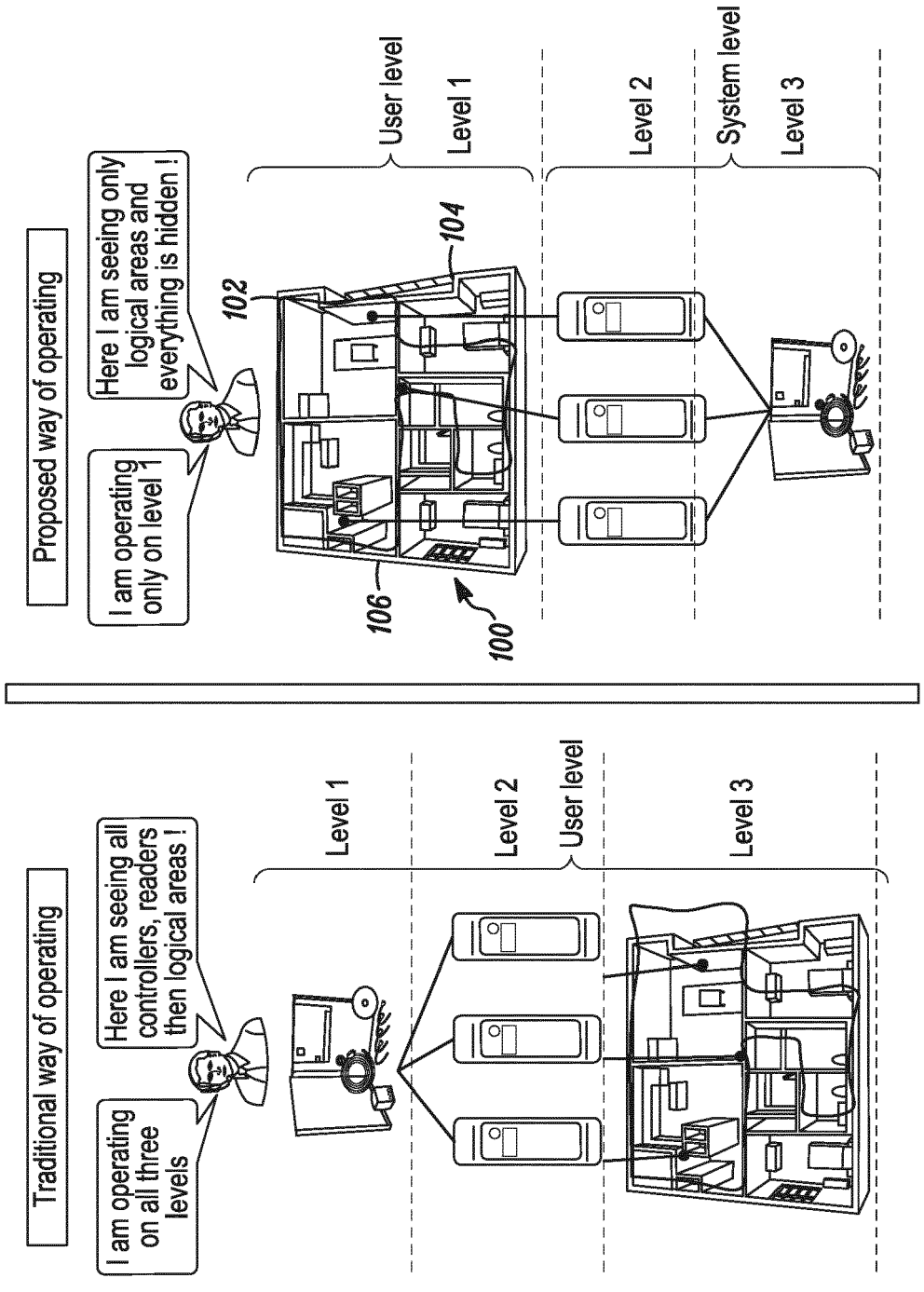

Traditional way of operating
I am operating on all three levels
Here I am seeing all controllers, readers then logical areas !
Level 1
Level 2
User level
Level 3
Proposed way of operating
I am operating only on level 1
Here I am seeing only logical areas and everything is hidden !
102
104
106
100
User level
Level 1
Level 2
System level
Level 3

FIG. 2A

FIG. 2B

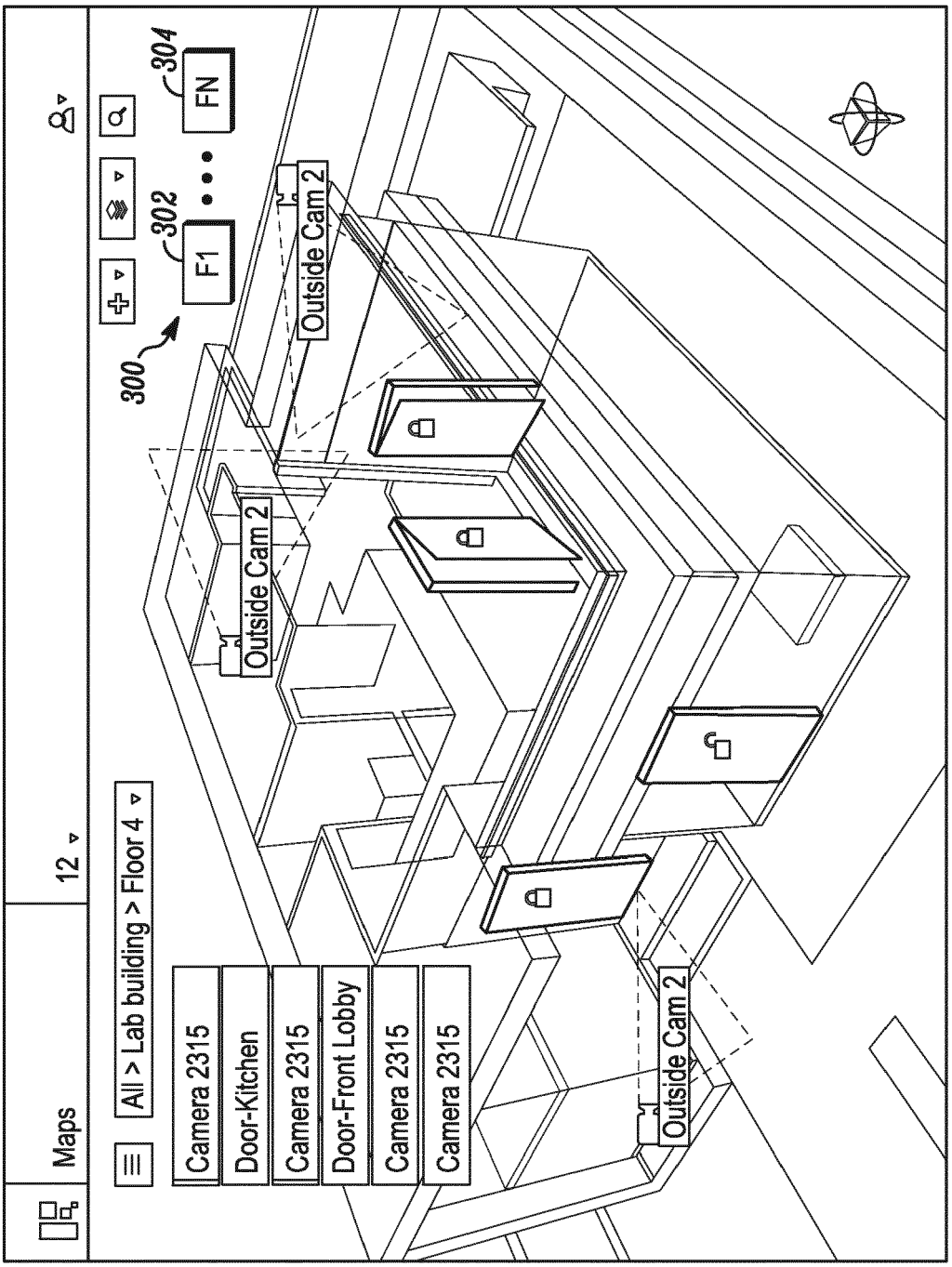
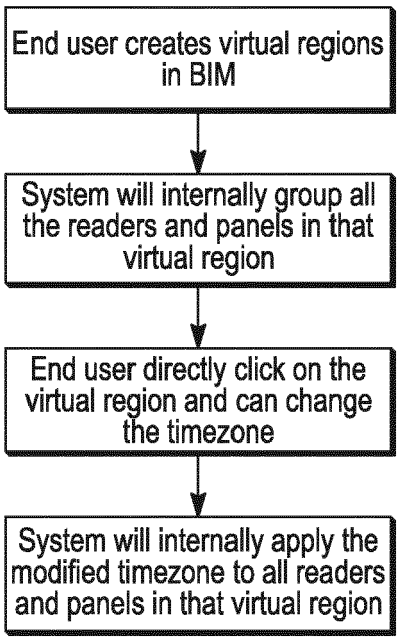
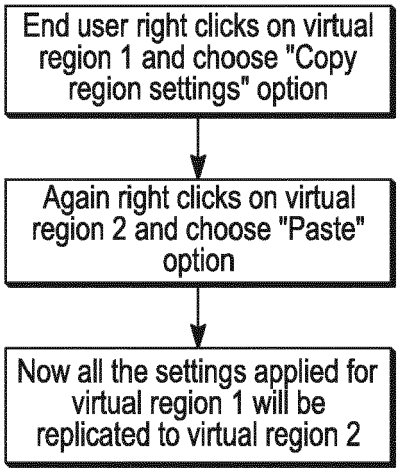

Maps
12
All > Lab building > Floor 4
Camera 2315
Door-Kitchen
Camera 2315
Door-Front Lobby
Camera 2315
Camera 2315
300
302
F1
304
FN
Outside Cam 2
Outside Cam 2
Outside Cam 2

FIG. 3



Time zone modification using proposed solution

FIG. 4



Copy/Paste rules and behavior settings using proposed solution

FIG. 5

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 14 17 9942

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	US 2007/219645 A1 (THOMAS ROBERT J [US] ET AL) 20 September 2007 (2007-09-20) * abstract; figures 1-7 * * paragraphs [0023] - [0045] *	1-15	INV. G06Q10/00 G08B25/14
X	US 2011/077754 A1 (JONES BRYAN [AU] ET AL) 31 March 2011 (2011-03-31) * abstract; figures 1-4 * * paragraphs [0007] - [0012], [0043] * * paragraphs [0054] - [0067] * * paragraphs [0072], [0081] *	1-15	
A	US 2012/133482 A1 (BHANDARI NEELENDRA [IN] ET AL) 31 May 2012 (2012-05-31) * abstract; figures 1,3a,3b * * paragraphs [0037] - [0041] * * paragraphs [0066] - [0076] *	1-15	

TECHNICAL FIELDS SEARCHED (IPC)

G05B
G08B
G07C
G06Q

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	9 January 2015	Buron, Emmanuel

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 14 17 9942

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

09-01-2015

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007219645 A1	20-09-2007	EP 1996982 A2	03-12-2008
		US 2007219645 A1	20-09-2007
		WO 2007109488 A2	27-09-2007
US 2011077754 A1	31-03-2011	NONE	
US 2012133482 A1	31-05-2012	EP 2408984 A1	25-01-2012
		US 2012133482 A1	31-05-2012
		WO 2010106474 A1	23-09-2010

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82